OIPE JC81
MAY 13 2004
PATENT & TRADEMARK OFFICE

PATENT

MS147672.1

CERTIFICATE OF MAILING

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-14501.

5-10-04
Date:

Himanshu S. Amin

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Applicant: Pradeep Bahl, *et al.*

Serial No: 09/587,204

Filing Date: June 5, 2000

Examiner: Alina A. Boutah

Art Unit: 2143

Title: SYSTEM AND METHOD FOR AUTOMATIC DETECTION AND CONFIGURATION OF NETWORK PARAMETERS

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

Applicants submit this brief in triplicate in connection with an appeal of the above-identified patent application. Please charge $330.00 for the fee associated with this brief to Deposit Account No. 50-1063[MSFTP108US].

I. Real Party in Interest (37 C.F.R. §1.192(c)(1))

The real party in interest in the present appeal is Microsoft Corporation, the assignee of the present application.

II. Related Appeals and Interferences (37 C.F.R. §1.192(c)(2))

Appellants, appellants' legal representatives, and/or the assignee of the present application are not aware of any appeals or interferences which will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §1.192(c)(3))

Claims 1-36 and 38-39 are pending in the subject application. The rejection of claims 1-36 and 38-39 is appealed.

IV. Status of Amendments (37 C.F.R. §1.192(c)(4))

No claim amendments have been entered subsequent the Final Office Action.

V. Summary of Invention (37 C.F.R. §1.192(c)(5))

The present invention relates to systems and methods that automatically configure a device's network parameters for a plurality of disparate networks prior to obtaining network addresses. (p.2, ll.15-16). More particularly, the present invention can be employed when a device is attached to a network, wherein the systems and methods query the network for network information (p.7, ll.12-23), search stored configurations for an associated network configuration (p.7, ll.24-28) and/or modify a stored configuration (p.10, ll.18-21), wherein a suitable (stored or modified) configuration is utilized to configure the device for network communication (p.7, ll.28-29) before a network address is provided (p.7, ll.9-14).

VI. Statement of the Issues (37 C.F.R. §1.192(c)(6))

A. Whether claim 1 is unpatentable under 35 U.S.C. §112, first paragraph, for lack of enablement.

B. Whether claims 1-6, 14-18, 22-34 and 38 are unpatentable under 35 U.S.C. §102(b) as being anticipated by Cheston, *et al.* (U.S. 6,412,025).

C. Whether claims 7-11, 35 and 39 are unpatentable under 35 U.S.C. §103(a) over Cheston, *et al.* (U.S. 6,412,025) in view of LeMaire, *et al.* (U.S. 5,999,530).

D. Whether claims 12-13, 19-21 and 36 are unpatentable under 35 U.S.C. §103(a) over Cheston, *et al.* (U.S. 6,412,025) in view of Romohr (U.S. 5,596,723).

VII. Grouping of Claims (37 C.F.R. §1.192(c)(7))

For the purposes of this appeal only, the claims are grouped as follows:

Claims 1-36 and 38-39 stand or fall together.

VIII. Argument (37 C.F.R. §1.192(c)(8))

A. Rejection of Claim 1 Under 35 U.S.C. §112, First Paragraph

Claim 1 stands rejected under 35 U.S.C. §112, first paragraph, for including subject matter that was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. In particular, it is asserted that it is unclear whether the "stored configuration" is located in the first or second computer system. It is respectfully submitted that this rejection should be withdrawn for at least the following reason. As disclosed at page 7, lines 24-29, (and in figures 1, 2, 3, 4a and 6 (configuration(s) 52, 52a and 52b)), the stored configuration(s) is associated with the first computer (computer 20). Accordingly, this rejection should be withdrawn.

B. Rejection of Claims 1-6, 14-18, 22-34, and 38 Under 35 U.S.C. §102(b)

Claims 1-6, 14-18, 22-34, 37 and 38 stand rejected under 35 U.S.C. §102(b) as being anticipated by Cheston, *et al.* (U.S. 6,412,025). It is respectfully submitted that this rejection should be withdrawn for at least the following reason. Cheston, *et al.* does not teach or suggest each and every aspect of the subject claims.

Claim 1

Independent claim 1 recites a first computer that configures a network interface based on ***modifying*** at least one stored configuration associated with received network information. Cheston, *et al.* does not teach or suggest such claimed aspects. Rather, Cheston, *et al.* discloses assigning a ***previous*** or ***new IP address*** upon attaching to a network. More particularly,

Cheston, *et al.* discloses that a ***previous IP address*** is utilized upon re-attaching to an entry point of a network or a ***new IP address*** is obtained when a new connection (*e.g.*, connecting to a different entry point) is established with the network. (*See* Abstract; col.4, ll.10-16; col.6, ll.38-52; Fig. 4). Cheston, *et al.* further discloses that a history log is updated with IP addresses such that the log provides a history of the previously and currently employed IP addresses. These logged IP addresses can be utilized upon re-attaching to the network. (*See* col.7, ll.4-14). In addition, new IP addresses can be obtained from DHCP when attaching to a new entry point. (*See* col.3, l.62 – col.4, l.29)

In contrast, the subject claim recites ***modifying*** at least one stored configuration associated with received network information in order to facilitate configuring a network interface. As disclosed in the subject application, a first computer (computer 20) can store network configurations and utilize the stored network configurations to set up the network interface. (*See* Application, p.7, ll.25-28). In instances where an associated stored configuration does not exist, the first computer can employ ***modifications of stored configurations*** to facilitate determining a suitable network configuration. (*See* Application, p.10, ll.17-18). Cheston, *et al.* is silent regarding employing modified stored configurations as recited in the subject claim.

The Examiner contends that Cheston, *et al.* discloses utilizing a modified stored configuration. For example, column 5, lines 25-33 of Cheston, *et al.* is referenced and provides "Cheston teaches a stored table of terminals attached to the server (interpreted as a second computer system) that is updated when a terminal is removed. In this case, the 'updated' information is interpreted as 'modified' stored configuration." (*See* Final Office Action, p.15). However, this quotation relates to a server-side table that can be utilized to identify ***terminals*** attached to the server (*See* Cheston, *et al.*, col.5, ll. 20-21), and does ***not*** disclose storing a network configuration, as recited in claim 1.

In addition, the Examiner states that he "interprets" ***updating*** the table of stored terminals to be synonymous with ***modifying*** stored network configurations, as recited in the subject claim. (*See* Final Office Action, p.15). However, Cheston, *et al.* defines updating the server-side table of terminals as ***removing*** pointers from the server-side table that are associated with a terminal no longer connected to a node (an old location) since such pointers are no longer valid and ***adding*** terminal information to the server-side table of terminals when attaching the terminal to a new node in order to indicate the new location. The foregoing is utilized when a terminal is

moved so that data is not misdirected to a removed terminal. (*See* Cheston, *et al.*, col.5, ll. 25-33). The Examiner references Cheston, *et al.*, col.3-4, ll.62-29 and figure 4 to support this contention. However, this section of Cheston, *et al.* simply discloses a system that "seeks" an IP address when it needs one, and does ***not*** teach or suggest configuring a network interface based on ***modifying*** at least one ***stored configuration***, as recited in the subject claim. From the foregoing, it is readily apparent that updating tables as taught in Cheston, *et al.* is ***not*** synonymous with ***modifying*** stored network configurations as recited in claim 1.

Claim 17

Independent claim 17 further recites a delay timer with a delay time ***based on a value of an associated address***. Cheston, *et al.* does not teach or suggest such aspects. The Examiner asserts that delay timers are inherent in systems that query networks. However, the Examiner does not provide any support for delay times that are ***based on a value of an associated address***, as recited in the subject claim. "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." (*See* MPEP §2112 *quoting Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990)). Since the Examiner does ***not*** address basing delay time on ***a value of an associated address***, it is submitted that he has not provided a sufficient basis in fact and/or technical reasoning to reasonably support an inherency assertion based on the teachings of Cheston, *et al.*.

Claim 24

Claim 24 recites means for configuring a network interface before a network identification has been established and based upon a response from the network. As disclosed in the subject specification, at least one means includes a first computer configuring a network interface based on modifying a stored configuration associated with received network information. As discussed *supra*, Cheston, *et al.* does not describe such novel aspects.

Claim 26

Independent claim 26 further recites a system comprising a multiple internet protocol configurations (MIPC) service that matches the at least one network configuration stored within the first computer with a network identification associated with the information received from the second computer, wherein the match facilitates the first computer in configuring a network interface. Cheston, *et al.* does not teach or suggest such features. Rather, Cheston, *et al.* simply discloses employing DHCP to provide an IP address in response to a request from a terminal. (*See* col. 3, lines 62-67).

It is asserted that a terminal's identification "must" be matched to IP addresses stored in the DHCP since Cheston, *et al.* does not seek a new IP address when a new IP address is not required. (*See* Final Office Action, p.16, Response to Arguments). However, the subject claim does not recite *requesting* an IP address from a DHCP or *receiving* an address therefrom. Instead, claim 26 recites matching network configuration stored within the first computer with a network identification associated with received network information. Cheston, *et al.* does not teach or suggest these claimed aspects; thus, Cheston, *et al.* does not teach each and every element of claim 26.

Claim 34

Independent claim 34 further recites the third computer system that determines a network configuration *via* communications from at least one of a first computer system and a second computer system. As disclosed in the subject application, the third computer system (other computers) can listen to network communications, for example, from the first computer system and/or the second computer system, and utilize this information to determine network configuration. (*See* Application, p.8, ll.7-14). Cheston, *et al.* does not teach or suggest such claimed aspects.

The Examiner contends that Cheston, *et al.* discloses such a system and references figure 3 to support this contention. However, this figure and the accompanying description are void of such aspects. In particular, the referenced section of Cheston, *et al.* simply provides an example of a typical network, wherein various computers are attached to one of a plurality of servers/routers, the servers/routers in turn are coupled to a host and a network; the referenced section of Cheston, *et al.* does not contemplate determining third computer system network

configuration from at least one of a first computer system and a second computer system, as recited in the subject claims.

In view of the above comments, it is respectfully requested that the rejection of independent claims 1, 17, 24, 26 and 34 (and claims 2-6 and 14-16, 18 and 22-23, 25, 27-33, and 38, which respectively depend therefrom) be withdrawn.

C. **Rejection of Claims 7-11, 35 and 39 Under 35 U.S.C. §103(a)**

Claims 7-11, 35 and 39 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cheston, *et al.* (U.S. 6,412,025) in view of LeMaire, *et al.* (U.S. 5,999,530). It is respectfully submitted that this rejection should be withdrawn for at least the following reason. Claims 7-11, 35 and 39 depend from independent claims 1 and 34, respectively, and LeMaire, *et al.* fails to make up for the aforementioned deficiencies of Cheston, *et al.* with respect to independent claims 1 and 34. *See In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed Cir. 1988) ("If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious."). Instead, Maire, *et al.* discloses a bridge that reduces unwanted WAN multicast packet traffic in a LAN *via* employing a filter based on information stored in a filtering database from WAN query and report packets and router-to-router packets. Accordingly, withdrawal of this rejection is requested.

D. **Rejection of Claims 12-13, 19-21 and 36 Under 35 U.S.C. §103(a)**

Claims 12-13, 19-21 and 36 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cheston, *et al.* (U.S. 6,412,025) in view of Romohr (U.S. 5,596,723). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Claims 12-13, 19-21 and 36 depend from independent claims 1, 17 and 34, respectively, and Romohr does not make up for the aforementioned deficiencies of Cheston, *et al.* with respect to independent claims 1, 17 and 34 (described *supra*). Rather, Romohr discloses a system that determines the most prevalent operating system services and protocols of a network and then configures itself accordingly. Since the combination of Cheston, *et al.* and Romohr does not teach or suggest ***all*** the limitations of the subject claims, it is respectively requested that the rejection of claims 12-13, 19-21 and 36 be withdrawn.

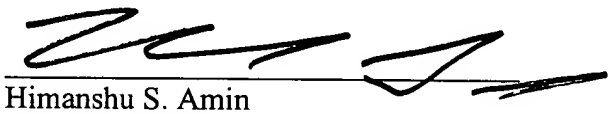
IX. Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejections of claims 1-36 and 38-39 be reversed.

If any additional fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063.

Respectfully submitted,

AMIN & TUROCY, LLP



Himanshu S. Amin
Reg. No. 40,894

AMIN & TUROCY, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114

Telephone (216) 696-8730
Facsimile (216) 696-8731

X. Appendix of Claims (37 C.F.R. §1.192(c)(9))

1. A system that automates detection and configuration of network parameters, comprising:

a first computer system that communicate with a network; and

at least a second computer system that provides network information, the first computer system queries the network and receives the network information from the at least a second computer system before a network identification has been established for the first computer system and the first computer configures a network interface based on modifications to at least one stored configuration and associated with the received network information.

2. The system of claim 1 further comprising a storage for storing the at least one configuration utilized to configure the network interface.

3. The system of claim 1, the first computer system configures the network interface by determining a network identification associated with the network information and matching the at least one configuration with the network identification.

4. The system of claim 1, the at least one configuration is determined from previous network configurations.

5. The system of claim 1, the at least one configuration is determined from previous static configurations.

6. The system of claim 1, the at least one configuration is determined from previous dynamic configurations.

7. The system of claim 1, the query is a multicast.

8. The system of claim 7, the multicast is addressed to a multicast Internet Protocol (IP) address.

9. The system of claim 8, the source IP address is 0.0.0.0.

10. The system of claim 7, the at least a second computer system responds to the multicast address *via* a Network Configuration Protocol (NCP) header.

11. The system of claim 10, the NCP header further comprises a subnet address and subnet mask.

12. The system of claim 1, the query is an Address Resolution Protocol (ARP) broadcast.

13. The system of claim 12, the ARP broadcast is associated with a router defined in the at least one configuration.

14. The system of claim 1, the first computer system interfaces to the network *via* at least one Network Interface Card (NIC).

15. The system of claim 1, the first computer system further comprises a timer for determining a time to receive the network information.

16. The system of claim 1, the at least a second computer system further comprises a timer for mitigating network traffic.

17. A method that automates detection and configuration of network parameters, comprising the steps of:

querying a network, the network comprising a plurality of network systems wherein respective network systems include a delay timer with a delay time based on a value of an associated address;

receiving a response from the network; and

configuring a network interface before a network identification has been established based upon the response from the network.

18. The method of claim 17, further comprising the steps of:
determining a network identification associated with the response; and
matching at least one configuration associated with the network identification.

19. The method of claim 17, the query is at least one of a multicast and a broadcast.

20. The method of claim 17, the query is an Address Resolution Protocol (ARP) broadcast.

21. The method of claim 17, the response is at least one of a multicast and a broadcast.

22. The method of claim 17, further comprising the step of starting a local timer to determine if a response has been received.

23. The method of claim 17, further comprising the step of starting at least one network system delay timer in order to mitigate network traffic.

24. A system that automates detection and configuration of network parameters, comprising:
means for querying a network;
means for receiving a response from the network; and
means for configuring a network interface before a network identification has been established based upon the response from the network.

25. The system of claim 24, further comprising:
means for determining a network identification associated with the response; and
means for matching at least one configuration associated with the network identification.

26. A system that automates detection and configuration of network parameters, comprising:

a first computer system with a network interface;

a storage that stores at least one configuration associated with a network;

at least a second computer system that provides network information to the first computer system; and

a Multiple Internet Protocol Configurations (MIPC) service that matches the at least one configuration with a network identification associated with the network information, wherein the first computer configures the network interface based on the matched configuration.

27. The system of claim 26, the Multiple Internet Protocol Configurations (MIPC) service comprising a set of configurations based on at least on one of past network configurations and predetermined configurations, the set utilized to the network identification.

28. The system of claim 26, the network interface is at least one Network Interface Card (NIC).

29. The system of claim 28, the NIC is mapped to the at least one configuration by the MIPC service.

30. The system of claim 29, the NIC is mapped *via* a binary table.

31. The system of claim 30, further comprising at least one configuration detector (CD) for providing an association between the NIC and the at least one configuration.

32. The system of claim 31, the configuration detector initiates a network operation by registering the network operation with the MIPC service.

33. The system of claim 26, the at least one configuration further comprises at least one of an Internet Protocol (IP) address, a subnet mask, a gateway address, a DHCP server, and a name server.

34. A system that automates detection and configuration of network parameters, comprising:

a first computer system having a network interface;

a storage that stores at least one configuration associated with a network;

a second computer system that provides network information; and

a third computer system without a network identification;

wherein the first computer system queries the second computer system *via* the network interface to receive the network information before a network identification has been established for the first computer system;

the first computer system configures the network interface by determining a network identification associated with the network information and matching the at least one configuration with the network identification.; and

the third computer system determines a network configuration *via* communications from at least one of the first computer system and the second computer system.

35. The system of claim 34, the query is a multicast.

36. The system of claim 34, the query is an Address Resolution Protocol (ARP) broadcast.

37. Cancelled

38. The system of claim 34, further comprising a router that transmits network configuration information periodically.

39. The system of claim 34, the query requests and responses are multicast over different addresses.